



DEPARTMENT OF THE ARMY
104TH AREA SUPPORT GROUP
UNIT 20193, BOX 0001
APO AE 09165-0001

REPLY TO
ATTENTION OF:

IMEU-HAN-IM

22 June 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy (CP) 3-3, Common Access Card (CAC) and Public Key Infrastructure (PKI) Usage

1. REFERENCES: AE Regulation 25-1-5, Public Key Infrastructure (PKI), AE Regulation 25-71.
2. PURPOSE. This policy defines the 104th Area Support Group (ASG) policy on the proper use of the CAC, when transmitting electronic messages.
3. APPLICABILITY. This policy applies to all civilian employees and military personnel assigned or attached to the 104th ASG Area of Responsibility (AOR).
4. DIGITAL SIGNATURES AND DIGITAL ENCRYPTION:

a. Information sent via e-mail over the LandWarNet (Unclass) is particularly vulnerable to compromise if it is not protected properly. PKI helps protect information sent via e-mail through the use of digital signatures and digital encryption.

(1) Digital Signatures. The digital signature enables senders to digitally "sign" messages using the certificate issued to them on their CAC. This capability is also used to digitally sign documents and provide authentication for access to Army Knowledge Online (AKO) and other Web sites according to AE Regulation 25-71. Digitally signing a message allows senders to send messages in a way that enables recipients to verify all of the following:

- (a) The message was sent by the individual identified as the sender.
- (b) The contents of the message were not changed after the message was digitally signed.
- (c) The sender cannot deny having sent the message (non-repudiation).
- (d) The sender's certificate has not expired or been revoked.

(2) Digital Encryption. Digital encryption allows senders to encrypt official information using PKI. To encrypt an e-mail message, the sender must obtain the public key of the intended recipient. E-mail users can obtain public keys by:

- (a) Addressing the official e-mail using the Army in Europe GAL.

IMEU-HAN-IM

SUBJECT: Command Policy (CP) 3-3, Common Access Card (CAC) and Public Key Infrastructure (PKI) Usage

(b) Saving the recipient's name in their Outlook Contacts list using a digitally signed e-mail from the recipient.

(c) Downloading the public key from the DOD PKI Directory (<https://dod411.chamb.disa.mil>) and saving the recipient's name in their Outlook Contacts list.

b. More information on digitally signing and encrypting e-mail messages is available at <https://iassure.usareur.army.mil/pki/cac.aspx>.

5. OFFICIAL INFORMATION REQUIRING DIGITAL SIGNATURE AND DIGITAL ENCRYPTION:

a. Digital Signature. Examples of some, but not all, official information that must be digitally signed when sent by e-mail within the Army in Europe and to other Army and DOD entities includes the following:

- (1) Budget and fiscal data.
- (2) Command directives that were initiated in the Defense Message System (DMS) and transferred to e-mail.
- (3) Command policy memorandums.
- (4) Contract data (for example, A-76 commercial activity bids and data for weapon systems).
- (5) Unclassified regular administrative and logistical reports.

b. Digital Signature and Digital Encryption. Examples of some, but not all, official information that must be digitally signed and encrypted when sent by e-mail within the Army in Europe include the following:

(1) Sensitive operational information. This information includes unclassified tactical, administrative, and logistical information that supports the warfighter according to the USAREUR Critical Information List (CIL) (for example, casualty reports, exercise deployment manning documents, information on installations and infrastructure, movement or transportation information, network data, unit status reports). NOTE: According to the USAREUR CIL (at [http://www.g3.hqusareur.army.smil.mil/divisions/plansdiv/infoops/opsec/CIL doc](http://www.g3.hqusareur.army.smil.mil/divisions/plansdiv/infoops/opsec/CIL%20doc)), the preferred means of sending unclassified information on operational matters is by classified e-mail message through the LandWarNet (Class). Personnel should send this information through the LandWarNet (Unclas) using an unclassified e-mail account only if they do not have a classified e-mail account.

IMEU-HAN-IM

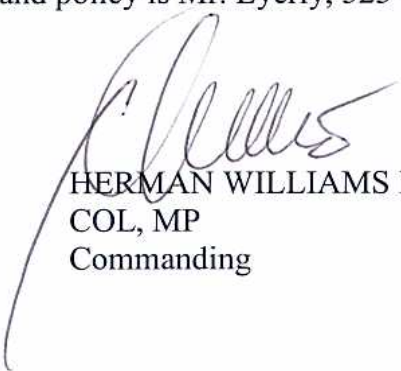
SUBJECT: Command Policy (CP) 3-3, Common Access Card (CAC) and Public Key Infrastructure (PKI) Usage

(2) Information marked For Official Use Only (FOUO).

(3) Medical care, personnel management, and Privacy Act data (including social security numbers).

NOTE: The Army in Europe is fully PK-enabled. Other component services and agencies in the European theater are becoming PK-enabled. Users should encourage organizations and users to become PK-enabled if they send or receive sensitive information under the provision of the USAREUR CIL.

6. Point of contact/proponent for this command policy is Mr. Eyerly, 323-3484.



HERMAN WILLIAMS III
COL, MP
Commanding

DISTRIBUTION:
"A"